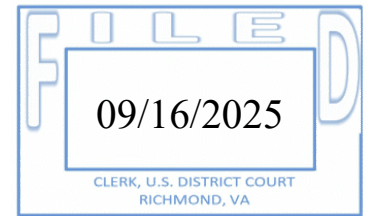


IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division



LISA WHITE, *individually and on behalf*)
of all others similarly situated,)
Plaintiff,)

v.)

THE UNITED NETWORK FOR ORGAN)
SHARING,)
Defendant.)

Civil Action No. 3:24CV629 (RCY)

MEMORANDUM OPINION

This is a putative class action stemming from Defendant United Network for Organ Sharing's ("UNOS") discovery that it had inadvertently stored private health information in a database available to unauthorized users for sixteen years. Plaintiff alleges that her private information was among the data inadvertently disclosed, which was then obtained and misused by malevolent third parties. The case is before the Court on Defendant's Motion to Dismiss Plaintiff's First Amended Complaint (the "Motion," ECF No. 21). The Motion has been fully briefed, and the Court dispenses with oral argument because the facts and legal contentions are adequately presented in the materials before the Court, and oral argument would not aid in the decisional process. E.D. Va. Loc. Civ. R. 7(J). For the reasons stated below, the Court will grant in part and deny in part Defendant's Motion.

I. BACKGROUND¹

A. Factual Allegations

Plaintiff Lisa White is a resident of Tennessee. Am. Compl. ¶ 25, ECF No. 19. Defendant United Network for Organ Sharing (“UNOS”) is a private corporation headquartered in Virginia that provides organ transplant services. *Id.* ¶¶ 26, 30. UNOS is funded through its federal contract as well as “computer registration fees paid by its members, including transplant hospitals and laboratories.” *Id.* ¶ 37.

1. Cybersecurity Landscape

In the last decade, the frequency and severity of data breaches have risen significantly. *See id.* ¶¶ 76–80. A record-high 1,862 data breaches occurred in 2021, surpassing the previous record of 1,506, set in 2017. *Id.* ¶ 76. In 2019 and 2020, six industry-leading private corporations experienced data breaches, including Microsoft, which resulted in the exposure of 250 million private records; and Facebook, which resulted in the exposure of 267 million users’ account information. *Id.* ¶ 78. Security experts anticipate increasing attacks from “social engineering and ransomware as nation-states and cyber criminals grow more sophisticated.” *Id.* ¶ 77. Most data breaches are preventable, and ultimately result from “misconfigurations, human error, poor maintenance, and unknown assets.” *Id.*

¹ When deciding a motion to dismiss under Rule 12(b)(6) of the Federal Rules of Civil Procedure, the Court “accept[s] as true the plaintiff’s well-pleaded allegations and views all facts and draws all reasonable inferences in the light most favorable to plaintiff.” *Philips v. Pitt Cnty. Mem’l Hosp.*, 572 F.3d 176, 180 (4th Cir. 2009). Such a standard, however, does not require accepting any unreasonable inferences or a plaintiff’s legal conclusions. *Id.* Additionally, a court may consider any documents attached to the complaint. *E.I. du Pont de Nemours & Co. v. Kolon Indus., Inc.*, 637 F.3d 435, 448 (4th Cir. 2011). Applying these standards, the Court construes the facts in the Complaint, including any attached documents, as follows. At the motion to dismiss stage, a court may consider the face of the complaint, documents attached to the complaint, documents attached to the motion to dismiss that are integral to the complaint and are authentic, and matters of public record subject to judicial notice. *Philips v. Pitt Cnty. Mem’l Hosp.*, 572 F.3d 176, 180 (4th Cir. 2009).

These same principles apply to a Rule 12(b)(1) facial challenge. *Beck v. McDonald*, 848 F.3d 262, 269–70 (4th Cir. 2017).

Cybercriminals create and exploit data breaches to obtain individuals’ personal identifiable information (“PII”). *Id.* ¶ 70. PII is then used to immediately defraud the victim or is repackaged and sold to others for the purpose of identity theft. *See id.* ¶¶ 70, 99–102. Because PII can be repackaged, it retains value on the black market well after a data breach occurs. *Id.* ¶ 122. PII is most valuable when it comprises a victim’s Social Security number, since Social Security numbers “are the key to stealing any person’s identity.” *Id.* ¶ 73. Armed with a victim’s Social Security number, a cybercriminal can “commit a broad range of fraud . . . , including obtaining employment; obtaining a loan; applying for credit cards or spending money; filing false tax returns; stealing Social Security and other government benefits; and applying for a driver’s license, birth certificate, or other public document.” *Id.* ¶ 119.

Victims of identity theft experience direct financial loss from the fraud perpetrated against them, as well as indirect losses by way of legal fees, bounced checks, and other associated expenses, such as utilizing “credit monitoring and identity theft protection services.” *Id.* ¶¶ 72, 118. Beyond that financial loss, however, victims also experience lost time, loss of privacy, and mental distress. *Id.* ¶¶ 118, 149.

Because it can be used to conduct lucrative fraud schemes, stolen consumer information is sold on the dark web “at a price ranging from \$40 to \$200.” *Id.* ¶ 87. “Criminals can also purchase access to entire company’s private data from \$900 to \$4,500.” *Id.* ¶ 88. Thus, Plaintiff contends that PII “is a valuable property right.” *Id.* ¶ 130.

Due to the frequency and risk of data breaches, “[c]ompanies that collect [PII] . . . are well aware of the risk of being targeted by cybercriminals.” *Id.* ¶ 70.

2. UNOS’s Data Collection and Breach

UNOS is the national administrator of the Organ Procurement and Transplantation Network (“OPTN”), which it operates “through a contract with the U.S. Department of Health and

Human Services.” Am. Compl. Ex. A (“Notice Letter”) at 1, ECF No. 19-1. In order to receive or provide an organ transplant, patients enter into contractual relationships with UNOS, in which they must provide UNOS with extremely sensitive private information, *e.g.*, Am. Compl. ¶¶ 34, 204, including: “Social Security numbers, dates of birth, health insurance claim numbers, the date information was added to the OPTN database, . . . other dates related to transplant or donor services,” *id.* ¶ 54, and “[e]xtensive lifetime medical information and [information regarding] comprehensive medical testing” (collectively, “Private Information”), *id.* ¶ 139. The Private Information is subject to UNOS’s Privacy Policy, which is provided to patients “upon the commencement of their medical transplant services relationship and upon request.” *Id.* ¶ 41.

In its Privacy Policy, UNOS promises the following:

[1] [T]he data we collect are securely stored on our servers according to industry standards and best practices for security;

[2] Any personally identifiable information you choose to provide is protected by privacy and security practices;

[3] [UNOS] does not disclose, give, sell, or transfer any personally identifiable information about our website visitors² unless required for law enforcement or by federal law.

Id. ¶¶ 38–41 (citation modified). After patients provide UNOS with their Private Information, UNOS stores it on the OPTN.³ *See, e.g., id.* ¶ 54. Alongside the OPTN database, UNOS also operates “the DonorNet system, which maintains the waitlist for all organ transplant candidates in the United States.” *Id.* ¶ 59.

² Because many of UNOS’s services are provided online “Plaintiff . . . w[as] among the UNOS’s website visitors.” Am. Compl. ¶ 40.

³ According to the Amended Complaint, UNOS self-reported that it stored “Social Security numbers, dates of birth, health insurance claim numbers, . . . and . . . dates related to transplant donor services” on OPTN. Am. Compl. ¶ 54. Plaintiff notes, however, that UNOS collected additional information from prospective organ donors and donees, including patients’ “lifetime medical information” as well as the results of “comprehensive medical testing.” *Id.* ¶ 139. Making all inferences in Plaintiff’s favor, the Court presumes that UNOS retained all of the preceding information on OPTN.

In 2007, UNOS launched a “test environment”: a purportedly distinct database populated with test data, *id.* ¶¶ 5, 49, in which “external system developers can test and demonstrate new tools and enhancements to the OPTN system,” *id.* ¶ 142. UNOS launched a second test environment in 2011. *Id.* ¶ 5. The test environments were accessible to anyone “employed by transplant hospitals, organ procurement organizations, and histocompatibility laboratory members, as well as third-party contractors for th[o]se . . . entities.” *Id.* ¶ 53.

Because of its status as a federal contractor, Congress took a particular interest in UNOS’s data security practices. *See id.* ¶ 59. Specifically, on January 31, 2022, the Senate Finance Committee wrote to UNOS “expressing concerns and asking then CEO Brian Shephard to take immediate action to modernize the national [OPTN] information technology system and secure it from cyber-attacks.”⁴ *Id.* ¶ 12 (citation modified). Then, on February 11, 2022, the Committee “wrote to the White House Chief Information Officer voicing [their] concerns about the cybersecurity and technology used by UNOS as the nation’s [OPTN] contractor.” *Id.*

On November 10, 2023, UNOS conducted two software tests of its databases. *Id.* ¶ 6. During those tests, UNOS discovered that it had accidentally populated the test environments with actual patients’ data—rather than test data—since their respective creation in 2007 and 2011 (“the Data Breach”). *See id.* ¶ 49; Notice Letter at 2 (“On November 10, 2023, the UNOS IT team discovered that users of the test environments had access to private information instead of test data. Due to a process error, private information has been stored in the test environments since their creation in 2007 and 2011.”). In other words, for sixteen years, anyone with access to the test environments could view any patients’ Private Information. *Id.* ¶¶ 5–7. And, because UNOS did not encrypt or redact any Private Information, third-party users of the test environments had

⁴ The Amended Complaint does not specify precisely what precipitated the Committee’s concern. *See generally* Am. Compl.

“unfettered access” to, *inter alia*, patients’ entire Social Security Numbers, alongside their full names and dates of birth, in plain violation of UNOS’s Privacy Policy. *Id.* ¶¶ 5, 65, 81–82.⁵

About ten months after its discovery of the Data Breach,⁶ *id.* ¶ 4, UNOS sent Notice of Data Breach Letters (“Notice Letter(s)”) to believed victims of the Data Breach, *id.* ¶ 3, advising them that their Private Information had been exposed to third parties.⁷ Notice Letter at 2.

3. Plaintiff White’s Experience

Plaintiff Lisa White began her relationship with UNOS when she registered as an organ donor in 2007. *Id.* ¶ 136. In exchange for the organ donation services, UNOS charged Plaintiff a fee, and required Plaintiff to provide an “extensive amount of her Private Information, including but not limited to her Social Security number, her health insurance information, and her lifetime medical history,” which was subject to its Privacy Policy. *Id.* ¶¶ 136, 204. At the outset of the relationship, Plaintiff was provided with a copy of UNOS’s Privacy Policy, which she reviewed and relied upon. *Id.* ¶¶ 41–42.

In July of 2009, Plaintiff was a kidney donor. *Id.* ¶ 137. Plaintiff believes that “additional Private Information was added to her [UNOS] file before and after the organ donation. *Id.* In

⁵ Plaintiff also alleges that UNOS did not employ other basic data security protocols, such as “scanning its system for exposed Private Information,” Am. Compl. ¶ 65; “[m]aintaining a secure firewall configuration”; or “[m]aintaining appropriate design, systems, and controls to limit user access to certain information as necessary,” *id.* ¶ 84.

⁶ Plaintiff alleges that this ten-month delay violated the HIPAA Breach Notification Rule (requiring notification within sixty days), the Tennessee Personal Consumer Information Release Act, and the Virginia Breach of Personal Information Notification Law (which prohibit unreasonable delay in notifying victims of data breach). Am. Compl. ¶ 56.

⁷ The Notice Letter also claimed that the exposed Private Information did not include patients’ names and had not been actually misused. Notice Letter at 2. These claims conflict with the allegations of the Amended Complaint. *Compare id.*, with Am. Compl. ¶¶ 47, 116, 119, 146, 150. In the instant Motion, UNOS argues that the Court should credit the statements of the Notice Letter over the allegations of the Amended Complaint. Def.’s Mem. Law Supp. Mot. Dismiss Pl.’s First Am. Compl. 5, ECF No. 22. However, the Court will not do so when an exhibit amounts to the unilateral statements of a defendant and conflicts with a plaintiff’s otherwise well-pleaded allegations. *Moody v. City of Newport News*, 93 F. Supp. 3d 516, 527 (E.D. Va. 2015) (“Rather than accepting every word in a unilateral writing by a defendant and attached by a plaintiff to a complaint as true, it is necessary to consider why a plaintiff attached the documents, who authored the documents, and the reliability of the documents.” (citation modified)).

addition, she believes that subsequent medical follow-up procedures and health data information may have been added to her UNOS file as recently as 2014.” *Id.*

As a general matter, Plaintiff is very careful not to share her Private Information, “especially as related to her medical history and organ donation as well as her Social Security number.” *Id.* ¶ 145. In fact, “[s]he has never knowingly transmitted unencrypted [personal information] over the internet or any other unsecured source” and has “refused to provide her Social Security number to any medical organizations for treatment even when asked.” *Id.*

Yet, in 2023, Plaintiff was notified by Experian that her entire Social Security number had been discovered on the dark web. *Id.* ¶ 146. Thereafter, Plaintiff began receiving notifications of fraudulent uses of her Social Security number. *Id.* In one instance, a credit card was fraudulently taken out in Plaintiff’s name. *Id.* In another, Plaintiff received notification that a fraudulent credit card application had been submitted in her name. *Id.* Each time Plaintiff receives such a notification, “she is forced to spend hours of time to stop and reverse the fraudulent activities.” *Id.*

Sometime in late August of 2024, Plaintiff received a Notice Letter from UNOS, notifying her that her Private Information, including her full Social Security number, had been exposed in the Data Breach. *Id.* ¶ 138. This notification caused Plaintiff significant distress, since she expected that the highly sensitive data associated with her kidney donation procedure “would be maintained in an *absolutely* secure manner.” *Id.* ¶ 141. Plaintiff contends that she “would not have provided UNOS with her Private Information” had she known that UNOS “lacked data security practices adequate to safeguard [Private Information], and that it would be so reckless to leave her Private Information unencrypted and exposed to unauthorized individuals.” *Id.* ¶ 142. As a result of the Data Breach, Plaintiff’s Private Information has been published to the dark web, which has already resulted in fraud against her. *See id.* ¶¶ 146–47. That fraud, in turn, has already cost Plaintiff her time and privacy. *Id.* ¶ 149. Plaintiff believes that, now that her Social Security

number is available to malevolent third parties, she will continue to face fraud attempts for the foreseeable future. *See id.* ¶ 151, 237. Further, Plaintiff believes that “UNOS’s data security measures remain inadequate,” which places her at even greater risk of further fraud. *Id.* ¶ 237.

B. Relevant Procedural History

Plaintiff filed her initial Complaint on September 5, 2024. Compl., ECF No. 1. Plaintiff filed her Amended Complaint on October 18, 2024. Am. Compl., ECF No. 19. On November 1, 2024, UNOS filed the instant Motion to Dismiss. Def.’s Mot. Dismiss, ECF No. 21; Def.’s Mem. Law Supp. Mot. Dismiss Pl.’s First Am. Compl. (“Mem. Supp. Mot. Dismiss”), ECF No. 22. On November 15, 2024, Plaintiff filed her Memorandum of Law in Opposition to Defendant’s Motion to Dismiss (“Memorandum in Opposition”), ECF No. 23. On November 21, 2024, UNOS filed its Reply in Support of its Motion to Dismiss Plaintiff’s First Amended Complaint (“Reply”), ECF No. 24. Accordingly, the Motion is now ripe for review.

II. LEGAL STANDARD

A. Article III Standing & Rule 12(b)(1)

Article III of the United States Constitution limits the jurisdiction of federal courts to “Cases” and “Controversies.” U.S. Const. art. III, § 2. “One element of the case-or-controversy requirement is that plaintiffs must establish that they have standing to sue.” *Clapper v. Amnesty Intern. USA*, 568 U.S. 398, 408 (2013) (citation modified). To establish standing, a plaintiff bears the burden of establishing the three “irreducible minimum requirements”:

(1) an injury-in-fact (i.e., a concrete and particularized invasion of a legally protected interest); (2) causation (i.e., a fairly traceable connection between the alleged injury in fact and the alleged conduct of the defendant); and (3) redressability (i.e., it is likely and not merely speculative that the plaintiff’s injury will be remedied by the relief plaintiff seeks in bringing suit).

David v. Alphin, 704 F.3d 327, 333 (4th Cir. 2013) (citation modified).

A standing challenge is a challenge to the Court’s subject matter jurisdiction and is therefore properly considered under Federal Rule of Civil Procedure 12(b)(1). *See, e.g., Beck v. McDonald*, 848 F.3d 262, 269–70 (4th Cir. 2017). The party asserting jurisdiction bears the burden of proving that federal jurisdiction is proper. *See Int’l Longshoremen’s Ass’n v. Va. Intern. Terminals, Inc.*, 914 F. Supp. 1335, 1338 (E.D. Va. 1996) (citing *McNutt v. Gen. Motors Acceptance Corp.*, 298 U.S. 178, 189 (1936); *Adams v. Bain*, 697 F.2d 1213, 1219 (4th Cir. 1982)). A Rule 12(b)(1) motion may challenge the existence of subject matter jurisdiction in one of two ways: facially or factually. *Beck*, 848 F.3d at 270; *Adams*, 697 F.2d at 1219. A facial challenge proceeds similarly to a Rule 12(b)(6) analysis, since “the defendant contends that a complaint simply fails to allege facts upon which subject matter jurisdiction can be based.” *Beck*, 848 F.3d at 270 (citation modified). Thus, in the context of a facial challenge, “the plaintiff is afforded the same procedural protection as she would receive under a Rule 12(b)(6) consideration, wherein the facts alleged in the complaint are taken as true, and the defendant’s challenge must be denied if the complaint alleges sufficient facts to invoke subject matter jurisdiction.” *Id.* at 270. Conversely, when faced with a factual challenge, the Court may weigh evidence presented by the parties to determine whether the undisputed facts support a finding of subject matter jurisdiction. *Evans v. B.F. Perkins Co.*, 166 F.3d 642, 647 (4th Cir. 1999).

B. Rule 12(b)(6)

“A motion to dismiss under Rule 12(b)(6) tests the sufficiency of a complaint; importantly, it does not resolve contests surrounding the facts, the merits of a claim, or the applicability of defenses.” *Megaro v. McCollum*, 66 F.4th 151, 157 (4th Cir. 2023) (quoting *Republican Party of N.C. v. Martin*, 980 F.2d 943, 952 (4th Cir. 1992)). Federal Rule of Civil Procedure 8 only requires that a complaint set forth “a short and plain statement of the claim showing that the pleader is entitled to relief,” in order to ‘give the defendant fair notice of what the . . . claim is and the grounds

upon which it rests.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (quoting *Conley v. Gibson*, 355 U.S. 41, 47 (1957)). While the complaint’s “[f]actual allegations must be enough to raise a right to relief above the speculative level,” “detailed factual allegations” are not required in order to satisfy the pleading requirement of Federal Rule 8(a)(2). *Id.* (citations omitted). The plaintiff’s well-pleaded allegations are assumed to be true, and the complaint is viewed in the light most favorable to the plaintiff. *Mylan Labs., Inc. v. Matkari*, 7 F.3d 1130, 1134 (4th Cir. 1993) (citations omitted); *see also Martin*, 980 F.2d at 952.

“To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 570). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.* (citing *Twombly*, 550 U.S. at 556). “The plausibility standard is not akin to a ‘probability requirement,’ but it asks for more than a sheer possibility that a defendant has acted unlawfully.” *Id.* “Labels and conclusions,” a “formulaic recitation of the elements,” and “naked assertions” without factual enhancement are insufficient. *Id.*

III. ANALYSIS

The Amended Complaint advances five claims against UNOS: (1) negligence, Am. Compl. ¶¶ 167–98, ECF No. 19; (2) breach of contract, *id.* ¶¶ 199–207; (3) breach of implied contract, *id.* ¶¶ 208–22; (4) unjust enrichment, *id.* ¶¶ 223–33; and (5) a request for declaratory judgement, *id.* ¶¶ 234–42. In the instant Motion, UNOS chiefly contends that Plaintiff’s claims against it must be dismissed because she lacks Article III standing. Mem. Supp. Mot. Dismiss 6–14, ECF No. 22. Alternatively, UNOS argues that Plaintiff fails to adequately allege each of the five claims against it. *Id.* at 14–20. For her part, Plaintiff contends that the allegations of the Amended Complaint

both establish standing and support each of the claims against UNOS. *See generally* Mem. Opp’n, ECF No. 23.

A. The Amended Complaint Adequately Alleges Article III Standing

The Court begins its analysis with UNOS’s contention that Plaintiff lacks standing to bring this action entirely. Citing a line of Fourth Circuit opinions considering Article III standing in the data breach context—*Beck*, *Hutton*, and *O’Leary*—UNOS advances a facial challenge of the sufficiency of the Amended Complaint. Mem. Supp. Mot. Dismiss 6. Specifically, it argues that Plaintiff has failed to allege the first two standing elements: injury and causation. *Id.* Largely relying on the same cases, Plaintiff contends that she has adequately alleged standing to sue. Mem. Opp’n 9–14.

1. Article III Standing Generally

As described above, Article III standing comprises three elements: (1) injury in fact; (2) causation; and (3) redressability. *E.g.*, *Beck*, 848 F.3d at 269–71. Here, UNOS contends that Plaintiff has failed to allege the first two elements. Mem. Supp. Mot. Dismiss 6.

In order to establish an injury in fact sufficient to support Article III standing, “a plaintiff must show that he or she suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical.” *Beck*, 848 F.3d at 270–71 (citation modified). Notably, a “threatened rather than actual injury can satisfy Article III standing requirements.” *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*, 204 F.3d 149, 160 (4th Cir. 2000) (en banc). Nevertheless, a plaintiff may not avail herself of a relaxed injury standard by simply alleging a threatened injury; in order to satisfy the demands of Article III, a threatened injury must be “concrete in both a qualitative and temporal sense” as well as “distinct and palpable,” and may not be “too speculative.” *Hutton v. Nat’l Bd. Exam’rs Optometry, Inc.*, 892 F.3d 613, 621 (4th Cir. 2018).

To satisfy the “causation” element of Article III standing, a plaintiff must allege a causal connection between the injury and the conduct complained of, such that one is “fairly traceable” to the other. *E.g., Hutton*, 892 F.3d at 623. Critically, the Fourth Circuit has “concluded that the fairly traceable standard is not equivalent to a requirement of tort causation.” *Id.*

2. Fourth Circuit Cases Considering Standing in the Data Breach Context

As noted by both parties, this case is decided in the shadow of three published Fourth Circuit opinions: *Beck*, *Hutton*, and *O’Leary*.

In *Beck v. McDonald*, 848 F.3d 262, 266–67 (4th Cir. 2017), the Fourth Circuit considered two consolidated appeals in which “the Plaintiffs sought to establish Article III standing based on the harm from the increased risk of future identity theft and the cost of measures to protect against it.” *Beck*, 892 F.3d at 266–67. The consolidated appeals stemmed from two data breaches of a veterans medical center. *Id.* at 267. In one case, the plaintiffs alleged that their personal information—including their names, birth dates, and last four digits of their Social Security numbers—had been saved to a laptop that was either misplaced by the defendant medical center or stolen. *Id.* at 267. Because of the nature of the data, the plaintiffs worried they were at risk of future identity theft, though there was no evidence that their data had been actually misused. *Id.* at 267–68. The other plaintiffs alleged that their full Social Security numbers were amongst documents stored in a box that had been misplaced or stolen. *Id.* at 268. They, like the other group of plaintiffs, were concerned that their information would be used to commit fraud against them, though there was no evidence that their information had yet been misused. *Id.* at 268–69.

Both of the *Beck* district courts held that the plaintiffs lacked standing. *Id.* at 266–67. The Fourth Circuit agreed that the consolidated plaintiffs’ unsubstantiated concern of future misuse

was simply too speculative,⁸ *Beck*, 892 F.3d at 274–75, and explained that “a mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft.” *Hutton*, 892 F.3d at 621 (describing the holding in *Beck*).

Just one year later, the Fourth Circuit decided *Hutton v. National Board of Examiners in Optometry*, 892 F.3d 613, 621–22 (4th Cir. 2018). There, the Fourth Circuit considered whether, in light of *Beck*, a group of optometrists had standing to pursue their claims against the defendant based on an alleged data breach. *Id.* at 616–17. The *Hutton* plaintiffs alleged that, in July 2016, credit card accounts had been fraudulently opened in their names. *Id.* at 617–18. None of them had received a formal data breach notification, but “determined that the only common source amongst them and to which they had all given their personal information . . . was the [defendant], where every graduating optometry student had to submit their personal information to sit for board-certifying exams.” *Id.* at 617. When the plaintiffs asked the defendant whether its information systems had been compromised, it initially denied the allegation, though later it sent the plaintiffs “a cryptic message stating its internal investigation was still ongoing . . . [and] advised the victims to remain vigilant in checking their credit.” *Id.* (citation modified). Applying *Beck*, the district court held that the plaintiffs had failed to adequately allege Article III standing. *Id.* at 619.

On appeal, the Fourth Circuit disagreed. Considering first the element of injury, the Fourth Circuit determined that the plaintiffs’ allegations plainly satisfied this element; in fact, the plaintiffs had articulated three cognizable theories of injury. *Id.* at 621–22. Where the *Beck* plaintiffs could only complain of a speculative threat of future data misuse, the *Hutton* plaintiffs “allege[d] that they have already suffered actual harm in the form of identity theft and credit card fraud.” *Id.* at 622. Such allegations of actual data misuse clearly constitute Article III injury-in-

⁸ The *Beck* court also declined to recognize the plaintiffs’ distress and cost of mitigative measures as independent Article III injuries, reasoning that these allegations were merely “a repackaged version of Plaintiffs’ first failed theory of standing.” *Beck*, 848 F.3d at 276–77.

fact. *Id.* Moreover, evidence of actual misuse gave rise to an inference of imminent *future* misuse. *Id.* at 622. Thus, the case could be sustained under a theory of injury-in-fact or future threatened injury. *See id.* Finally, the court determined that, because the plaintiffs had alleged a non-speculative injury, standing could also be premised “on the basis of costs incurred to mitigate or avoid harm.” *Id.* (“[T]he Court has recognized standing to sue on the basis of costs incurred to mitigate or avoid harm when a substantial risk of harm actually exists”). Thus, the plaintiffs’ allegations demonstrated three theories of injury: (1) injury-in-fact based on actual data misuse; (2) sufficiently imminent risk of future data misuse; and (3) injury-in-fact based on mitigation costs.

Finding that the plaintiffs had articulated an Article III injury, the *Hutton* court moved to Article III’s causation prong. *Id.* at 624. There, the court determined that the plaintiffs’ allegations adequately supported an inference that the fraud resulted from a breach of the defendants’ systems, emphasizing that, at the pleading stage, such allegations need only be “plausible on their face.” *Id.* at 624. Accordingly, the Fourth Circuit determined that the *Hutton* plaintiffs had adequately alleged Article III standing, reversing the district court’s decision.⁹

Approximately five years after *Hutton*, the Fourth Circuit decided *O’Leary v. TrustedID*, 60 F.4th 240, 241 (4th Cir. 2023). Unlike the plaintiffs in *Beck* and *Hutton*, the *O’Leary* plaintiff had not been subject to a known or suspected data breach. *Id.* Instead, the *O’Leary* plaintiff sought relief under a state statute that prohibited internet businesses from asking consumers for all or part of their Social Security numbers. *O’Leary*, 60 F. 4th at 241. The plaintiff alleged that the defendant had violated this statute and then shared his Social Security number with Equifax. *Id.* The plaintiff argued that the defendant’s choice to share his Social Security number placed

⁹ As is the case here, the third Article III standing element—redressability—was not in dispute. *Hutton*, 892 F.3d at 624.

him at a heightened risk of identity theft, since Equifax had previously been subject to cyberattacks. *Id.* at 245. Notwithstanding this purportedly heightened risk, the Fourth Circuit held that the plaintiff had not alleged a sufficiently imminent risk that he would be subject to data theft, since the possibility of such an outcome required the court to engage in “[a] daisy chain of speculation.” *Id.* Thus, because the plaintiff had not alleged that his data had been actually misused, and because he had not adequately alleged a sufficiently imminent risk of future misuse, the Fourth Circuit determined that the plaintiff lacked standing. *Id.*

3. This Case is Most Like *Hutton*

Applying *Beck*, *Hutton*, and *O’Leary* to the instant matter, it is clear to the Court that Plaintiff’s allegations are most akin to the facts of *Hutton*; in fact, Plaintiff has alleged an Article III injury fairly traceable to the conduct of UNOS with even more clarity than the plaintiffs in *Hutton*. Therefore, the Court finds that Plaintiff has adequately alleged Article III standing.

First, under the logic of *Hutton*, Plaintiff has plainly alleged three cognizable Article III injuries. Here, like *Hutton*, and unlike *Beck* and *O’Leary*, Plaintiff alleges that her data has been *actually misused*: Plaintiff’s Private Information has been allegedly coopted by malevolent third-parties and used to apply for and acquire credit cards in Plaintiff’s name. Am. Compl. ¶ 146. Thus, Plaintiff has “been concretely injured . . . [and] there is no need to speculate on whether substantial harm will befall [Plaintiff].” *Hutton*, 892 F.3d at 622. Applying the logic of *Hutton*, the fact that Plaintiff’s data has already been misused also gives rise to a reasonable inference that there is a substantial risk her data will be further misused in the future, *id.*, particularly since Experian has alerted her that her data is for sale on the dark web, Am. Compl. ¶ 146. Finally, under *Hutton*, Plaintiff also has “standing to sue on the basis of costs incurred to mitigate or avoid harm [since] a substantial risk of harm actually exists.” *Hutton*, 892 F.3d at 622. Thus, like the plaintiffs in *Hutton*, Plaintiff has established three theories of injury cognizable under Article III:

an injury-in-fact based on the misuse of her data, a sufficiently imminent threatened injury based on risk of future misuse, and injury-in-fact based on mitigation efforts. *See id.* at 621–23.

The Court also finds that Plaintiff has adequately alleged that her injuries are fairly traceable to the conduct of UNOS, satisfying the causation element of standing. In *Hutton*, the Fourth Circuit held that plaintiffs had established Article III causation because they had alleged facts sufficient to give rise to a plausible inference that the fraud perpetrated against them resulted from a breach of the defendant’s information systems, even when the defendant refused to confirm or deny whether its systems had, in fact, been breached. *Hutton*, 892 F.3d at 623.

Similarly to *Hutton*, Plaintiff’s allegations give rise to a plausible inference that the misuse of her information resulted from the Data Breach. Here, Plaintiff alleges that, as a general matter, she refrains from sharing her Private Information, particularly her Social Security number. Am. Compl. ¶ 145. Yet, in 2023, she began receiving notifications from Experian that her Social Security number had been compromised, resulting in at least two instances of attempted fraud. *Id.* ¶ 146. Then, in 2024, UNOS notified Plaintiff that it had inadvertently exposed her Private Information to unauthorized users continuously for sixteen years. *Id.* ¶ 138. These allegations give rise to an inference that Plaintiff’s injuries resulted from the Data Breach with even more conviction than the inference of *Hutton*, since UNOS has admitted to the Data Breach. As such, the Court finds that Plaintiff has adequately alleged Article III causation. Because this resolves both of UNOS’s standing challenges, the Court will deny this portion of UNOS’s Motion advanced under Rule 12(b)(1).¹⁰

¹⁰ Plaintiff also contends that her loss of privacy constitutes an Article III injury. Mem. Opp’n 15–17. Because the Court has found that Plaintiff otherwise articulates Article III standing, it does not reach this argument.

B. Plaintiff Adequately Alleges Negligence by UNOS

Following its argument that Plaintiff lacks standing, UNOS argues that Plaintiff fails to state each element of her negligence claim. Mem. Supp. Mot. Dismiss 14–16. Specifically, UNOS alleges that it owed no duty to Plaintiff to protect her information, and, therefore, Plaintiff fails to allege that it acted in a negligent manner. *Id.* at 14–15. UNOS also contends that, even if it behaved negligently, Plaintiff cannot plausibly contend that its conduct was the proximate cause of any fraud against her, since Plaintiff can only speculate that the misuse of her data actually resulted from the Data Breach. *Id.* at 15–16. Plaintiff disagrees. Mem. Opp’n 19–22. Specifically, she argues that UNOS assumed a duty to behave carefully with regards to her private information, which it breached by failing to adequately program and screen its systems. *Id.* at 19–21. Thus, Plaintiff contends that UNOS’s negligence proximately caused the actual misuse of her data. *Id.* at 22–23. The Court agrees with Plaintiff and will deny this aspect of UNOS’s Motion.

In Virginia,¹¹ “the elements of an action in negligence are a legal duty on the part of the defendant, breach of that duty, and a showing that such breach was the proximate cause of injury, resulting in damage to the plaintiff.” *Willner v. Dimon*, 849 F.3d 93, 113 (4th Cir. 2017) (applying Virginia law) (citation modified). All persons owe a general duty to act in a manner that will not injure others. *E.g., Quisenberry v. Huntington Ingalls Inc.*, 818 S.E.2d 805, 809–10 (Va. 2018). Whether a defendant had a duty to act in a particular manner—or to refrain from acting in a particular manner—can be determined by weighing the risk of injury and the gravity of a possible injury against the burden imposed by protecting against the injury. *E.g., Dodson v. Kleffman*, 912 S.E.2d 499, 521 (Va. Ct. App. 2025). “Virginia has [also] recognized the concept of assumption

¹¹ Both parties presume that Virginia law controls Plaintiff’s state law claims. *See generally* Mem. Supp. Mot. Dismiss; Mem. Opp’n. Indeed, while Plaintiff resides in Tennessee, Am. Compl. ¶ 25, this Court applies the choice of law rules of the state in which it sits; Virginia, in turn, “applies the *lex loci delicti*, the law of the place of the wrong, to tort actions.” *Milton v. IIT Rsch. Ins.*, 138 F.3d 519, 521 (4th Cir. 1998). Here, the *lex loci delicti* is the law of Virginia, since UNOS is organized and headquartered in Richmond, Virginia. Am. Compl. ¶ 26.

of duty: ‘one who assumes to act, even though gratuitously, may thereby become subject to the duty of acting carefully, if he acts at all.’” *In re Capital One Cons. Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 399 (E.D. Va. 2020) [hereinafter *In re Capital One*] (quoting *Kellermann v. McDonough*, 684 S.E.2d 781, 791 (Va. 2009)). A defendant only assumes a duty as to a plaintiff, however, when the defendant “personally engage[d] in some affirmative act amounting to a rendering of services to another.” *Id.* (citation modified).

Of course, to prevail in a negligence claim, the plaintiff must also show the second element of negligence: that the defendant in fact breached the relevant duty. *E.g.*, *Sturman v. Johnson*, 163 S.E.2d 170, 176 (1968). As to the third element, the plaintiff must show that the defendant’s conduct proximately caused the plaintiff’s injuries. *Scott v. Simms*, 51 S.E.2d 250, 254 (Va. 1949). A plaintiff demonstrates an adequate causal link “if an ordinary, careful and prudent person ought, under the circumstances, to have foreseen that an injury might probably result from the negligent act.” *Id.*

First, the Court finds that Plaintiff has adequately alleged that UNOS assumed a duty of care regarding her Private Information, satisfying the first element of a negligence claim. Here, Plaintiff alleges that UNOS solicited Plaintiff’s information as a pre-condition to participation in its organ donation program. Am. Compl. ¶¶ 136, 204. In *In re Capital One*, another Court in this district considered analogous facts as applied to a Virginia negligence claim. 488 F. Supp. 3d at 399. There, the plaintiffs alleged that the defendant had solicited their data in exchange for credit card services and then stored the data in a cloud environment that, due to a misconfiguration error, was particularly vulnerable to cyberattack. *Id.* at 388–89. The *In re Capital One* court reasoned that such conduct amounted to an assumption of duty on the defendant’s part, since the defendant had actively solicited the plaintiffs’ data as a precondition to its credit card services. *Id.* at 399–

400. Thus, the plaintiffs had adequately alleged that the defendant bore a duty to behave carefully with regards to storage and maintenance of their data.

The critical allegations supporting a finding that the *In re Capital One* defendant had assumed a duty to care for the plaintiffs' data are also present here. As in *In re Capital One*, UNOS actively solicited Plaintiff's Private Information as a precondition to participation in its organ donation services. Am. Compl. ¶¶ 136, 204. Thus, under the logic of *In re Capital One*, UNOS undertook a duty to maintain Plaintiff's Private Information with care. Accordingly, Plaintiff has adequately alleged the first element of her negligence claim.

As to the second element of her negligence claim, the Court readily finds that Plaintiff has plausibly alleged that UNOS did not behave with care as to the maintenance of her Private Information, constituting a breach of its assumed duty. As described above, a party breaches its duty when it fails to use ordinary care; ordinary care, in turn, can be ascertained by considering the likelihood of the relevant injury and the gravity of a potential injury in light of the burden imposed by protecting against an injury. *Dodson*, 912 S.E.2d at 521.

According to the allegations of the Amended Complaint, data breaches are prolific amongst organizations who storehouse consumer data, which almost invariably results in data misuse—the exact injury which Plaintiff complains of here. Am. Compl. ¶¶ 70–77. The likelihood of such an injury occurring is made significantly worse when an organization misconfigures its systems or fails to upkeep them. *Id.* ¶ 77. Data misuse is a significant injury, particularly when the relevant data includes consumer Social Security numbers, since Social Security numbers can be used to “commit a broad range of fraud” against a victim. *Id.* ¶¶ 73, 119. Given the high risk and severity of such an injury, careful organizations redact or encrypt consumer data, protect their equipment and computer files, scan their system for exposed consumer data, and practice proper structuring and monitoring of their collected data. *Id.* ¶¶ 65, 84, 147. Here, however, Plaintiff alleges that

UNOS took no such action; in fact, UNOS allegedly stored patients' unencrypted, unredacted, highly sensitive Private Information in a database made available to unauthorized parties for *sixteen years*. Am. Compl. ¶¶ 5–7, 65, 81–82. If proven, this level of inaction clearly constitutes a breach of UNOS's duty of care. Accordingly, Plaintiff has adequately alleged the second element of a negligence claim.

As to the third element of her negligence claim, the Court finds that Plaintiff has plausibly alleged that UNOS's conduct, as outlined above, proximately caused the misuse of her Private Information. Proximate cause, notwithstanding its moniker, does not require close temporal proximity between the conduct of a tortfeasor and a resulting injury. *See Scott*, 51 S.E.2d at 254. Instead, a defendant's conduct proximately causes an injury whenever “an ordinary, careful and prudent person ought, under the circumstances, to have foreseen that an injury might probably result from the negligent act.” *Id.* As emphasized above, data breaches are a common occurrence, particularly when an organization, like UNOS, storehouses a significant amount of consumer data. Am. Compl. ¶¶ 70–77. And, it is certainly foreseeable that, if a data breach were to occur, malevolent actors would exploit that breach to commit fraud and other data misuse. *See id.* ¶ 118. Such an outcome is especially predictable when the relevant organization fails to protect against such an injury by, *inter alia*, encrypting or redacting consumer information—as UNOS allegedly failed to do here. *See id.* ¶ 147. Thus, based on the sheer nature of its organization and its failure to encrypt or redact patients' Private Information, the misuse of patients' Private Information is a natural and probable result of UNOS's conduct. Accordingly, Plaintiff has plausibly alleged that UNOS's conduct proximately caused the misuse of her data.

As a result of the foregoing, the Court finds that Plaintiff has adequately stated her negligence claim and will deny this aspect of UNOS's Motion.

C. Plaintiff Adequately Alleges Her Breach of Contract Claim

Next, UNOS contends that Plaintiff fails to state her breach of contract claim because she has not adequately alleged a contractual relationship between herself and UNOS. Mem. Supp. Mot. Dismiss 16. Plaintiff argues that she has. Mem. Opp’n 22. Here, the Court again agrees with Plaintiff.

In order to state a claim for breach of contract in Virginia, a plaintiff must allege: “(1) a legally enforceable obligation of a defendant to a plaintiff; (2) the defendant's violation or breach of that obligation; and (3) injury or damage to the plaintiff caused by the breach of obligation.” *MCR Fed., LLC v. JB&A, Inc.*, 808 S.E.2d 186, 195 (Va. 2017). A party has a legally enforceable obligation to another when the parties have entered into a contractual relationship, which follows the “mutual assent of the contracting parties to terms reasonably certain,” *Allen v. Aetna Cas. & Sur. Co.*, 281 S.E.2d 818, 820 (Va. 1981), and the exchange of valuable consideration, *Smith v. Mountjoy*, 694 S.E.2d 598, 602 (Va. 2010). The Virginia Supreme Court defines consideration as follows:

Consideration may arise from any act done at the defendant’s request, and for his convenience, or at the inconvenience of the plaintiff. . . . It may be in the form of a benefit to the party promising or a detriment to the party to whom the promise is made.

Id.

Here, Plaintiff alleges that, in 2007, she entered into an agreement with UNOS, in which she agreed to provide UNOS a registration fee and her Private Information in exchange for participation in the organ donation program. Am. Compl. ¶¶ 34, 136, 204. Plaintiff further alleges that the Privacy Policy was provided to patients “upon the commencement of their medical transplant services relationship,” and therefore was incorporated into the parties’ agreement. *Id.* ¶ 41. Thus, Plaintiff alleges that, at the outset of her relationship with UNOS, she reviewed and

relied upon the Privacy Policy. *Id.* ¶¶ 41–42. By way of the Privacy Policy, UNOS promised Plaintiff:

[1] [T]he data we collect are securely stored on our servers according to industry standards and best practices for security;

[2] Any personally identifiable information you choose to provide is protected by privacy and security practices;

[3] [UNOS] does not disclose, give, sell, or transfer any personally identifiable information about our website visitors¹² unless required for law enforcement or by federal law.

Id. ¶¶ 38–41 (citation modified). Because many of UNOS’s services are online, Plaintiff was among UNOS’s website visitors. *Id.* ¶ 40. During the period of the Data Breach, UNOS violated its Privacy Policy by, at the very least, disclosing personal identifiable information about Plaintiff to the third-party users of the test environments. *E.g., id.* ¶¶ 5–7, 49.

UNOS contends that Plaintiff fails to state the first two elements of a breach of contract claim: that UNOS had obligations to Plaintiff at all, and that those obligations included the commitments of the Privacy Policy. Mem. Supp. Mot. Dismiss 16. It does not contest that the Data Breach, as alleged, constituted a breach of the Privacy Policy. *See generally id.*

The Court disagrees. At this juncture, Plaintiff has plausibly alleged the existence of a contractual relationship between herself and UNOS that incorporated the commitments of the Privacy Policy. First, Plaintiff plainly and plausibly alleges mutual assent: Plaintiff alleges that she agreed with UNOS to provide her Private Information as an aspect of her participation in the organ donation process, and that their agreement incorporated the Privacy Policy. Am. Compl. ¶¶ 34, 41, 136, 204. This assent was accompanied by consideration, since Plaintiff exchanged her Private Information and a registration fee for the use of UNOS’s organ donation services. *Id.*; *see*

¹² Because many of UNOS’s services are provided online “Plaintiff . . . w[as] among the UNOS’s website visitors.” Am. Compl. ¶ 40.

Smith, 694 S.E.2d at 602. At the outset of this relationship with UNOS, Plaintiff reviewed and relied upon the Privacy Policy. *Id.* ¶¶ 41–42. Thus, Plaintiff has plausibly alleged a contractual relationship between herself and UNOS that incorporated the Privacy Policy. And, because there is no contest that she has likewise alleged that the Data Breach amounted to a violation of the Privacy Policy, the Court finds that she has adequately stated her breach of contract claim.

UNOS’s arguments do not upset this conclusion. UNOS contends that Plaintiff’s breach of contract claim fails because it relies on a theory “contrary to Fourth Circuit law.” Mem. Supp. Mot. Dismiss 16. In support, UNOS cites *J.R. v. Walgreens Boots Alliance* (“*Walgreens*”), an unpublished Fourth Circuit opinion, in which the Fourth Circuit held that the plaintiffs had failed to plausibly allege that they had entered into a contract with the defendant that incorporated the defendant’s privacy policy. 2021 WL 4859603, at *5–6 (4th Cir. Oct. 19, 2021). The Fourth Circuit came to this conclusion because the privacy policy did not itself constitute a contract; it merely recited the company’s legal duties and privacy practices, and there were no other allegations demonstrating an agreement between the parties. *Id.* at *1–2.

As an unpublished opinion, the rule of *Walgreens* does not bind this Court. However, even if it did, the factual allegations at bar are critically distinct from those in *Walgreens*. Here, unlike in *Walgreens*, Plaintiff alleges that there existed a broader agreement between herself and UNOS, which incorporated the Privacy Policy. And, unlike the privacy policy in *Walgreens*, UNOS’s Privacy Policy made specific commitments regarding its treatment of Plaintiff’s Private Information, beyond its basic legal obligations. Am. Compl. ¶¶ 38–41. These distinctions go to the heart of a breach of contract claim and therefore dictate a different outcome here.

As a result, and notwithstanding UNOS's arguments to the contrary, the Court concludes that Plaintiff has adequately stated her breach of contract claim.¹³

D. Plaintiff has Adequately Stated her Implied Contract Claim

UNOS next proceeds to Plaintiff's breach of implied contract claim. Incorporating its previous argument that Plaintiff has failed to allege an agreement between herself and UNOS, UNOS contends that Plaintiff's implied contract claim also fails. Mem. Supp. Mot. Dismiss 16–19. Plaintiff contends otherwise, Mem. Opp'n 23–26, to which the Court agrees.

Virginia law “distinguishes between two types of implied contracts: contracts that are implied-in-fact and contracts that are implied-in-law.” *Rosetta Stone Ltd. v. Google, Inc.*, 676 F.3d 144, 166 (4th Cir. 2012). Here, Plaintiff advances an implied-in-fact theory. Mem. Opp'n 23. “Implied-in-fact contracts are no different from express contracts except that, instead of all of the terms and conditions being expressed between the parties, some of the terms and conditions are implied in law from the conduct of the parties.” *Spectra-4, LLP v. Uniwest Com. Realty, Inc.*, 772 S.E.2d 290, 293 (Va. 2015) (citation modified). Thus, a breach of implied contract claim requires the claimant to allege the same elements as are necessary to state a claim for breach of an express contract. *Rosetta Stone Ltd.*, 676 F.3d at 166.

Because the Court has already concluded that Plaintiff has plausibly alleged that UNOS breached an express contract between them, *supra* Part III.C, the shared standard between the two claims dictates the same result here. *See In re Capital One*, 488 F. Supp. 3d at 413–14 (permitting the plaintiffs' implied contract claim to survive based on previous analysis of express contract

¹³ Plaintiff also argues that her breach of contract claim could proceed under a theory of unilateral contract formation. Mem. Opp'n 23. Because the Court has found that Plaintiff plausibly alleges a traditional contractual relationship between herself and UNOS, it expresses no opinion as to whether Plaintiff plausibly states a claim of unilateral contract breach.

claim). Thus, for the reasons stated above, the Court finds that Plaintiff has adequately stated her implied contract claim.¹⁴

E. Plaintiff Fails to State a Claim of Unjust Enrichment

Next, UNOS argues that Plaintiff has failed to state her unjust enrichment claim because it “never promised to prove data security to Plaintiff”; thus, even in light of the Data Breach, it is not “unjust” for UNOS to retain any benefit conferred by Plaintiff.¹⁵ Mem. Supp. Mot. Dismiss 17–19. In response, Plaintiff contends the very opposite—considering the Data Breach, it is unfair for UNOS to benefit from Plaintiff’s paid fee and the value of her Private Information. Mem. Opp’n 24–25. Here, the Court agrees with UNOS.

Unlike contracts implied in fact, “implied-in-law contracts (also called “quasi-contracts”) do not stem from an actual agreement between the parties; rather, they are “a remedy imposed by the court.” *Doe v. Wash. & Lee Univ.*, 439 F. Supp. 3d 784, 791 (W.D. Va. 2020) (citation modified). Unjust enrichment claims are a category of implied-in-law contracts. *Po River Water & Sewer Co. v. Indian Acres Club, Inc.*, 495 S.E.2d 478, 482 (Va. 1998) (“To avoid unjust enrichment, equity will effect a contract implied in law, requiring one who accepts and receives the services of another to make reasonable compensation for those services.” (citation modified)). A *prima facie* case of unjust enrichment is comprised of three elements: “(1) plaintiff conferred a benefit on defendant; (2) defendant knew of the benefit and should reasonably have expected to repay plaintiff; and (3) defendant accepted or retained the benefit without paying for its value.”

¹⁴ Notably, an express agreement between two parties will supersede an implied contract claims. *In re Capital One*, 488 F. Supp. 3d at 413–14. Thus, as this case progresses, the Court will consider Plaintiff’s implied contract claim as an alternative claim pursuant to Federal Rule of Civil Procedure 8(d)(2).

¹⁵ UNOS also argues that, as a factual matter, it was not unjustly enriched because it did not charge Plaintiff monies for the organ donation services. Mem. Supp. Mot. Dismiss 17–18. Because this contradicts the well-pleaded allegations of the Amended Complaint, Am. Compl. ¶ 224, the Court rejects this aspect of UNOS’s argument. *Philips*, 572 F.3d at 180 (explaining that, in the context of a Rule 12(b)(6) motion, courts must “accept as true the plaintiff’s well-pleaded allegations”).

T. Musgrove Construction Co. v. Young, 840 S.E.2d 337, 341 (Va. 2020). Critically, “[o]ne may not recover under a theory of implied contract simply by showing a benefit to the defendant, without adducing other facts to raise an implication that the defendant promised to pay the plaintiff for such benefit.” *Nedrich v. Jones*, 429 S.E.2d 201, 207 (Va. 1993).

Here, Plaintiff contends that she conferred benefits to UNOS by paying it a fee and providing her Private Information. *E.g.*, Am. Compl. ¶ 224. In support of her unjust enrichment claim, she argues that UNOS “should have applied a portion of said monies received towards securing Plaintiff’s [Private Information] but did not.” Mem. Opp’n 26. Thus, Plaintiff contends that it is unfair for UNOS to retain the benefits conferred by Plaintiff. *Id.*

Some level of unfairness, however, is insufficient to sustain a claim of unjust enrichment. Instead, a plaintiff must plausibly allege that the defendant should have reasonably expected to pay the plaintiff for the benefit conferred. *E.g.*, *Rosetta Stone v. Google*, 676 F.3d 144, 166 (4th Cir. 2012) ; *Lugo v. Inova Health Care Servs.*, 2025 WL 905191, at *5 (E.D. Va. Mar. 25, 2025). The Amended Complaint lacks allegations that would give rise to an inference that UNOS should have expected to either pay Plaintiff for her Private Information or refund her fee upon the occurrence of a Data Breach. Indeed, Plaintiff alleges that some entities *would* pay money for her Private Information. Am. Compl. ¶ 87. There is no reason to believe, however, that either party expected an organization such as UNOS to pay for her information in conjunction with organ donation services. Likewise, there is no reason to believe that either party should have expected that UNOS would repay the fee upon a Data Breach. *Cf. Rosetta Stone*, 676 F.3d at 166; *Lugo*, 2025 WL 905191, at *5. Accordingly, the Court finds that Plaintiff has failed to state her unjust enrichment claim and will grant this aspect of UNOS’s Motion.¹⁶

¹⁶ Notably, this conclusion diverges from that of *In re Capital One*, upon which Plaintiff chiefly relies. Mem. Opp’n 24. There, the court held that:

F. Plaintiff's Declaratory Judgment Claim is Adequately Alleged and Otherwise Appropriate

Finally, UNOS contends that the Court should dismiss Plaintiff's declaratory judgment claim. Mem. Supp. Mot. Dismiss 17. In response, Plaintiff contends that her request for declaratory judgment is appropriate because it is derivative of her substantive claims. Mem. Opp'n 26. The Court agrees with Plaintiff.

The Declaratory Judgment Act permits district courts, "[i]n . . . case[s] of actual controversy within [their] jurisdiction," to "declare the rights and other legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought." 28 U.S.C. § 2201(a). However, the Supreme Court has "repeatedly characterized the Declaratory Judgment Act as 'an enabling Act, which confers a discretion on the courts rather than an absolute right upon the litigant.'" *Wilton v. Seven Falls Co.*, 515 U.S. 277, 287 (1995) (quoting *Pub. Serv. Comm'n of Utah v. Wycoff Co.*, 344 U.S. 237, 241 (1952)). However, a district court's discretion in deciding whether to entertain a declaratory judgment action is not boundless. *See Volvo Constr. Equip. N. Am., Inc. v. CLM Equip. Co.*, 386 F.3d 584, 594 (4th Cir. 2004). Rather, "[a] district court must have 'good reason' for declining to exercise its declaratory judgment jurisdiction." *Id.* (quoting *Cont'l Cas. Co. v. Fuscardo*, 35 F.3d 963, 965 (4th Cir. 1994)).

Here, Plaintiff asks the Court to declare UNOS's continuing obligation to secure patients' Private Information and to timely notify of any future data breach, and that UNOS continues to

the failure to secure a party's data can give rise to an unjust enrichment claim where a defendant accepts the benefits accompanying plaintiff's data and does so at the plaintiff's expense by not implementing adequate safeguards, thereby making it "inequitable and unconscionable" to permit defendant to retain the benefit of the data (and any benefits received therefrom), while leaving the plaintiff party to live with the consequences.

In re Capital One, 488 F. Supp. 3d at 412. In this portion of its analysis, however, the *In re Capital One* court relied only on New York and Minnesota case law. *See id.* This stands in contrast to the above-cited negligence analysis, *supra* Part III.B., which applied Virginia law. *In re Capital One*, 488 F. Supp. 3d at 399. Accordingly, the Court respectfully declines to apply this portion of *In re Capital One* to the instant analysis.

breach its legal duty by “failing to employ reasonable measures to secure consumers’ Private Information.” Am. Compl. ¶ 238.

First, the Court finds that there exists an actual controversy between the parties; therefore, the declaratory judgment claim is adequately alleged. Plaintiff and UNOS clearly dispute UNOS’s obligations regarding patients’ Private Information as well as the present state of UNOS’s data security measures: the two matters about which Plaintiff seeks declaratory relief. *Compare* Am. Compl. ¶¶ 237, 240 (alleging that UNOS’s data security measures remain inadequate), *with* Mem. Supp. Mot. Dismiss 19 (contending that, as a factual matter, Plaintiff is not at risk of any future harm); *see also* Mem. Supp. Mot. Dismiss 3 n.1 (dismissing Plaintiff’s allegation that UNOS had an obligation to timely notify victims of the Data Breach as “random”). Accordingly, Plaintiff’s declaratory judgment claim is adequately alleged. Thus, the only remaining question is whether the Court, in its discretion, will permit Plaintiff to pursue this claim. Finding that declaratory relief would be helpful to clarify the rights of the parties, the Court will permit Plaintiff to do so.

As noted above, the Declaratory Judgment Act confers discretionary power to Article III courts. *E.g., Wilton*, 515 U.S. at 287. However, that discretion is cabined by the requirement that “[a] district court must have ‘good reason’ for declining to exercise its declaratory judgment jurisdiction.” *Volvo Contr. Equip. N. Am., Inc.*, 386 F.3d at 594.

The Fourth Circuit has held that district courts should hear a “declaratory judgment action when declaratory relief ‘will serve a useful purpose in clarifying and settling the legal relations in issue,’ and ‘will terminate and afford relief from the uncertainty, insecurity, and controversy giving rise to the proceeding.’” *Id.* (quoting *Aetna Cas. & Sur. Co. v. Quarles*, 92 F.2d 321, 325 (4th Cir. 1937)). Conversely, this Court has held that declaratory judgment is inappropriate where the plaintiff “seek[s] to remedy past behavior rather than prevent future harm,” or where a declaration

would render “essentially identical relief” as another claim in the complaint. *Summit Invs. II v. Sam’s East*, 2024 WL 1223541, at *13 (E.D. Va. Mar. 21, 2024) (citation modified).


The Court finds no good reason to decline to hear Plaintiff’s declaratory judgment claim here. As demonstrated by the extent of the dispute between the parties, a declaratory judgment would clearly clarify their respective rights. Moreover, the particular declaration sought by Plaintiff, Am. Compl. ¶ 238, would certainly afford relief from her “uncertainty” and “insecurity” as to the risk of future exposure of her Private Information. Accordingly, the Court will permit Plaintiff’s declaratory judgment claim to proceed.

As such, the Court will deny Defendant’s Motion as to Plaintiff’s declaratory judgment claim.

IV. CONCLUSION

For the reasons detailed above, Defendant’s Motion to Dismiss will be granted in part and denied in part.

An appropriate Order shall issue.

/s/ 

Roderick C. Young
United States District Judge

Date: September 16, 2025
Richmond, Virginia